[h2] **What is Claimed is:**

[1 (c1)]
A method for authorizing requested processing by an adjunct program module, the method comprising:

receiving a request from a requesting module;
receiving a certificate from the requesting module;
determining whether the certificate authorizes processing in response to the request; and
processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

[2 (c2)]
The method of Claim_1 wherein determining comprises:

verifying a signature of the certificate by a certificate authority.

[3 (c3)]
The method of Claim_1 wherein determining comprises:

determining that the requesting module owns the certificate.

[4 (c4)]
The method of Claim_3 wherein determining that the requesting module owns the certificate comprises:

sending test data to the requesting module; and
receiving response data from the requesting module wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

[5 (c5)]
The method of Claim_4 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

[6 (c6)]
The method of Claim_4 wherein the response data includes a cryptographic signature of the test data.

[7 (c7)]
The method of Claim_4 wherein the test data is encrypted according to the certificate.

[8 (c8)]
The method of Claim_7 wherein the test data is encrypted using a public key of the certificate.

[9 (c9)]
The method of Claim_7 wherein the response data is decrypted from the test data.

[10 (c10)]
The method of Claim 4 wherein determining further comprises:
generating the test data randomly.

[11 (c11)]
The method of Claim 1 wherein determining comprises:
determining that the certificate includes data specifying one or more types of actions permitted by the certificate; and
determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

[12 (c12)]
The method of Claim 1 wherein the adjunct program module is a module in a dynamic link library.

[13 (c13)]
A method for authorizing requested processing by an adjunct program module, the method comprising:
receiving a request from a requesting module;
receiving an authorization interface from the requesting module;
requesting authorization from the requesting module according to the authorization interface;
receiving authorization data in response to the requesting authorization;
determining whether the authorization data authorizes processing in response to the request; and
processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

[14 (c14)]
The method of Claim 13 wherein the authorization data includes a certificate.

[15 (c15)]
The method of Claim 14 wherein determining comprises:
verifying a signature of the certificate by a certificate authority.

[16 (c16)]
The method of Claim 14 wherein determining comprises:
determining that the requesting module owns the certificate.

[17 (c17)]
The method of Claim 13 wherein requesting authorization comprises:
sending test data to the requesting module; and
further wherein the authorization data includes response data wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

[18 (c18)]
The method of Claim 17 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

[19 (c19)]
The method of Claim 17 wherein the response data includes a cryptographic signature of the test data.

[20 (c20)]
The method of Claim 17 wherein the test data is encrypted according to the certificate.

[21 (c21)]
The method of Claim 20 wherein the test data is encrypted using a public key of the certificate.

[22 (c22)]
The method of Claim 20 wherein the response data is decrypted from the test data.

[23 (c23)]
The method of Claim 17 wherein sending test data further comprises:
generating the test data randomly.

[24 (c24)]
The method of Claim 13 wherein determining comprises:
determining that the authorization data includes data specifying one or more types of actions permitted by the certificate; and
determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

[25 (c25)]
The method of Claim 13 wherein the adjunct program module is a module in a dynamic link library.

[26 (c26)]
A computer readable medium useful in association with a computer which includes a processor and a memory, the computer readable medium including computer instructions which are configured to cause the computer to authorize requested processing by an adjunct program module by:
receiving a request from a requesting module;
receiving a certificate from the requesting module;
determining whether the certificate authorizes processing in response to the request; and
processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

[27 (c27)]
The computer readable medium of Claim 26 wherein determining comprises:
verifying a signature of the certificate by a certificate authority.

[28 (c28)]
The computer readable medium of Claim 26 wherein determining comprises:
determining that the requesting module owns the certificate.

[29 (c29)]
The computer readable medium of Claim 28 wherein determining that the requesting module owns the certificate comprises:
sending test data to the requesting module; and
receiving response data from the requesting module wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

[30 (c30)]
The computer readable medium of Claim 29 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

[31 (c31)]
The computer readable medium of Claim 29 wherein the response data includes a cryptographic signature of the test data.

[32 (c32)]
The computer readable medium of Claim 29 wherein the test data is encrypted according to the certificate.

[33 (c33)]
The computer readable medium of Claim 32 wherein the test data is encrypted using a public key of the certificate.

[34 (c34)]
The computer readable medium of Claim 32 wherein the response data is decrypted from the test data.

[35 (c35)]
The computer readable medium of Claim 29 wherein determining further comprises:
generating the test data randomly.

[36 (c36)]
The computer readable medium of Claim 26 wherein determining comprises:
determining that the certificate includes data specifying one or more types of actions permitted by the certificate; and
determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

[37 (c37)]
The computer readable medium of Claim 26 wherein the adjunct program module is a module in a dynamic link library.

[38 (c38)]
A computer readable medium useful in association with a computer which includes a processor and a memory, the computer readable medium including computer instructions which are configured to cause the computer to authorize requested processing by an adjunct program module by:

receiving a request from a requesting module;
receiving an authorization interface from the requesting module;
requesting authorization from the requesting module according to the authorization interface;
receiving authorization data in response to the requesting authorization;
determining whether the authorization data authorizes processing in response to the request; and
processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

[39 (c39)]
The computer readable medium of Claim 38 wherein the authorization data includes a certificate.

[40 (c40)]
The computer readable medium of Claim 39 wherein determining comprises:

verifying a signature of the certificate by a certificate authority.

[41 (c41)]
The computer readable medium of Claim 39 wherein determining comprises:

determining that the requesting module owns the certificate.

[42 (c42)]
The computer readable medium of Claim 38 wherein requesting authorization comprises:

sending test data to the requesting module; and
further wherein the authorization data includes response data wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

[43 (c43)]
The computer readable medium of Claim 42 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

[44 (c44)]
The computer readable medium of Claim 42 wherein the response data includes a cryptographic signature of the test data.

[45 (c45)]

The computer readable medium of Claim 42 wherein the test data is encrypted according to the certificate.

[46 (c46)]
The computer readable medium of Claim 45 wherein the test data is encrypted using a public key of the certificate.

[47 (c47)]
The computer readable medium of Claim 45 wherein the response data is decrypted from the test data.

[48 (c48)]
The computer readable medium of Claim 42 wherein sending test data further comprises:
generating the test data randomly.

[49 (c49)]
The computer readable medium of Claim 38 wherein determining comprises:
determining that the authorization data includes data specifying one or more types of actions permitted by the certificate; and
determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

[50 (c50)]
The computer readable medium of Claim 38 wherein the adjunct program module is a module in a dynamic link library.

[51 (c51)]
A computer system comprising:
a processor;
a memory operatively coupled to the processor; and
a processing authorization module (i) which executes in the processor from the memory and (ii) which, when executed by the processor, causes the computer to authorize requested processing by an adjunct program module by:

receiving a request from a requesting module;
receiving a certificate from the requesting module;
determining whether the certificate authorizes processing in response to the request; and
processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

[52 (c52)]
The computer system of Claim 51 wherein determining comprises:
verifying a signature of the certificate by a certificate authority.

[53 (c53)]
The computer system of Claim 51 wherein determining comprises:
determining that the requesting module owns the certificate.

[54 (c54)]
The computer system of Claim 53 wherein determining that the requesting module owns the certificate comprises:
sending test data to the requesting module; and
receiving response data from the requesting module wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

[55 (c55)]
The computer system of Claim 54 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

[56 (c56)]
The computer system of Claim 54 wherein the response data includes a cryptographic signature of the test data.

[57 (c57)]
The computer system of Claim 54 wherein the test data is encrypted according to the certificate.

[58 (c58)]
The computer system of Claim 57 wherein the test data is encrypted using a public key of the certificate.

[59 (c59)]
The computer system of Claim 57 wherein the response data is decrypted from the test data.

[60 (c60)]
The computer system of Claim 54 wherein determining further comprises:
generating the test data randomly.

[61 (c61)]
The computer system of Claim 51 wherein determining comprises:
determining that the certificate includes data specifying one or more types of actions permitted by the certificate; and
determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

[62 (c62)]
The computer system of Claim 51 wherein the adjunct program module is a module in a dynamic link library.

[63 (c63)]
A computer system comprising:

a processor;
a memory operatively coupled to the processor; and
a processing authorization module (i) which executes in the processor from the memory and (ii) which, when executed by the processor, causes the computer to authorize requested processing by an adjunct program module by:
receiving a request from a requesting module;
receiving an authorization interface from the requesting module;
requesting authorization from the requesting module according to the authorization interface;
receiving authorization data in response to the requesting authorization;
determining whether the authorization data authorizes processing in response to the request; and
processing according to programming of the adjunct program module in response to the request upon a condition in which the certificate authorizes processing in response to the request.

[64 (c64)]
The computer system of Claim 63 wherein the authorization data includes a certificate.

[65 (c65)]
The computer system of Claim 64 wherein determining comprises:
verifying a signature of the certificate by a certificate authority.

[66 (c66)]
The computer system of Claim 64 wherein determining comprises:
determining that the requesting module owns the certificate.

[67 (c67)]
The computer system of Claim 63 wherein requesting authorization comprises:
sending test data to the requesting module; and
further wherein the authorization data includes response data wherein the response data is derived from the test data in a manner which requires ownership of the certificate.

[68 (c68)]
The computer system of Claim 67 wherein the response data is derived from the test data in a manner which requires access to a private key which is associated with the certificate.

[69 (c69)]
The computer system of Claim 67 wherein the response data includes a cryptographic signature of the test data.

[70 (c70)]
The computer system of Claim 67 wherein the test data is encrypted according to the certificate.

[71 (c71)]
The computer system of Claim 70 wherein the test data is encrypted using a public key of the

certificate.

[72 (c72)]
The computer system of Claim 70 wherein the response data is decrypted from the test data.

[73 (c73)]
The computer system of Claim 67 wherein sending test data further comprises:
generating the test data randomly.

[74 (c74)]
The computer system of Claim 63 wherein determining comprises:
determining that the authorization data includes data specifying one or more types of actions permitted by the certificate; and
determining that the one or more types of actions includes at least one type of action associated with processing to be performed in response to the request.

[75 (c75)]
The computer system of Claim 63 wherein the adjunct program module is a module in a dynamic link library.

[h3] **Abstract of the Disclosure**

[p65] To provide improved security in adjunct program modules such as plug-ins and dynamic link libraries, a requesting module provides an authorization interface to the invoked module such that the invoked module can require a certificate of the requesting module and can also challenge the authority of the requesting module. The certificate can include one or more permissions which are prerequisites for processing by the invoked module. The invoked module can challenge the authority of the requesting module by sending random test data to the requesting module and receiving in response a cryptographic signature of the test data. By verifying the signature of the requesting module using the received certificate, the invoked module confirms that the requesting module is, in fact, the owner of the receive certificate.

[h7] **Figures**